Peak Event Fraud Readiness Checklist for Fraud & Risk Operations Teams

High-risk, high-volume events create the perfect conditions for fraud. Traffic surges, operational pressure increases, and attackers use the noise to hide coordinated abuse.

This checklist outlines how teams can prepare for peak periods without forcing a tradeoff between fraud prevention and customer experience. The goal is to keep trusted users moving, detect abuse earlier, and adapt protections in real time as attack patterns shift.

Before the Event

- **Identify moments most likely to create fraud pressure**
  Launches, flash sales, seasonal peaks, limited inventory drops, loyalty promotions, and live events often attract spikes in both traffic and attacker activity.
- **Prepare to automate decisions at scale**
  Ensure manual review does not become the operational bottleneck when login and transaction volume increases.
- **Define where step-up authentication should apply**
  Map authentication and verification triggers to high-risk behaviors such as suspicious logins, account changes, new payment methods, high-value purchases, or unusual device activity.
- **Protect the full customer journey, not just checkout**
  Review protections across account creation, login, checkout, payments, stored value, refunds, and payouts.
- **Align teams on escalation paths before traffic spikes**
  Ensure fraud, engineering, operations, and support teams know who owns critical decisions, how incidents escalate, and when controls should tighten or relax.

See how Sift helps businesses prepare for peak fraud events

REQUEST A DEMO

Peak Event Fraud Readiness Checklist for Fraud & Risk Operations Teams

During the Surge

- ❒ **Keep trusted users moving with low-friction experiences**
  Apply additional verification only when risk signals justify it, not broadly across all users.
- ❒ **Watch for coordinated attacks hiding inside traffic spikes**
  Monitor for account takeover (ATO), bot activity, credential stuffing, card testing, promo abuse, and multi-accounting.
- ❒ **Monitor operational and fraud performance in real time**
  Track approval rates, block rates, manual review queues, authentication challenges, velocity anomalies, and behavioral shifts.
- ❒ **Adjust protections dynamically as attack patterns evolve**
  Avoid broadly tightening controls for all users. Target friction based on risk signals and suspicious behavior patterns.
- ❒ **Use behavioral, device, network, and velocity intelligence to detect threats earlier**
  Earlier detection reduces fraud exposure before attackers can scale activity or complete high-value transactions.

After the Event

- ❒ **Review fraud and operational performance**
  Analyze changes in fraud attack rates, false positives, approval rates, customer friction, and manual review volume.
- ❒ **Watch for delayed disputes and chargebacks**
  Compromised accounts and high-risk transactions often surface days or weeks after the event window closes.
- ❒ **Document lessons learned and optimization opportunities**
  Identify which controls worked effectively, where friction was unnecessary, and what should change before the next peak event.
- ❒ **Use event insights to strengthen future fraud strategy**
  Every peak event creates valuable intelligence that can improve policies, workflows, and response strategies moving forward.

What Sift Enables

- ✓ **Real-time decisioning at peak scale**
  Make highly accurate fraud decisions in under 150ms so trusted users can move quickly even during high-volume events.
- ✓ **Dynamic, risk-based friction**
  Apply step-up authentication only when risk warrants it to reduce unnecessary customer friction while protecting revenue.
- ✓ **Adaptive protection across the full customer journey**
  Protect every stage of the user lifecycle, from account creation and login to checkout, stored value, refunds, and payouts.
- ✓ **Operational resilience during traffic surges**
  Reduce manual review bottlenecks and give fraud teams the visibility and controls needed to respond faster as threats evolve.
- ✓ **Post-event analytics and optimization**
  Analyze policy decisions, attack patterns, operational performance, and outcomes so every event strengthens future fraud strategy.

See how Sift helps businesses prepare for peak fraud events

REQUEST A DEMO

sift